'I make up a silly name': Understanding Children's Perception of Privacy Risks Online

Jun Zhao
jun.zhao@cs.ox.ac.uk
Department of Computer Science.
University of Oxford
Oxford, UK

Ge Wang
ge.wang.17@ucl.ac.uk
Department of Information Studies.
University College London
London, UK

Carys Dally
carysdally@gmail.com
Department of Experimental
Psychology. University of Oxford
Oxford, UK

Petr Slovak[*]
p.slovak@ucl.ac.uk
Department of Informatics,
King's College London
London, UK

Julian Edbrooke-Childs[†]
Julian.Childs@annafreud.org
UCL Interaction Centre, University
College London
London, UK

Max Van Kleek
Nigel Shadbolt
max.van.kleek@cs.ox.ac.uk
nigel.shadbolt@cs.ox.ac.uk
Department of Computer Science.
University of Oxford
Oxford, UK

ABSTRACT

Children under 11 are often regarded as too young to comprehend the implications of online privacy. Perhaps as a result, little research has focused on younger kids' risk recognition and coping. Such knowledge is, however, critical for designing efficient safeguarding mechanisms for this age group. Through 12 focus group studies with 29 children aged 6-10 from UK schools, we examined how children described privacy risks related to their use of tablet computers and what information was used by them to identify threats. We found that children could identify and articulate certain privacy risks well, such as information oversharing or revealing real identities online; however, they had less awareness with respect to other risks, such as online tracking or game promotions. Our findings offer promising directions for supporting children's awareness of cyber risks and the ability to protect themselves online.

[*] Also with UCL Interaction Centre, University College London.
[†] Also with Anna Freud National Centre for Children & Families.

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300336

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; **Privacy protections**.

KEYWORDS

Privacy, Family Technologies, Children, Tablet Computers, Scaffolding

ACM Reference Format:
Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3290605.3300336

1 INTRODUCTION

Today, children are spending more time online than with other media sources, such as watching television or playing offline video games [48, 60]. Among the many kinds of devices now connected to the Internet, mobile devices (such as tablet computers or smartphones) have become the primary means by which children go online [48]. In the UK, 44% of children aged five to ten have been provided with their own tablets, with this percentage increasing annually [60], while in the US, ownership of tablets by children in this age group grew fivefold between 2011 and 2013 [1]. Children under five are also using smartphone and tablets more often, as the category of apps designed for younger kids continues to expand rapidly [6, 60].

Whilst online content has opened up significant new opportunities and experiences for children to learn and have fun [39, 58, 63, 67], parents and educators alike are raising concerns about the rapid adoption of online content and apps by children, in particular as it relates to the amount of time spent online, and online safety [36, 40, 47]. A recent survey has shown that parents consider privacy their primary concern regarding their children's use of the Internet [47]. This concern is driven, in part, by the view that children themselves are too young to understand the privacy risks they might face [45, 49], which drives many parents to take a restrictive approach to filter or monitor their children's online activity [41, 83]. Indeed, recent studies show how children's ability to recognise risks online remains inadequate, and as a result, the children are dependent on parents' strategies to keep them safe [41, 48, 50, 83]. Unfortunately, however, parents themselves often feel they lack an adequate understanding of the landscape of potential risks online—ranging from bullying to cybercrime—making them uncertain about the effectiveness of their mediation approaches [49].

We feel that it is important to understand children's privacy behaviours and conceptualisations not only because it might identify conceptual gaps in understanding that lead to better ways to educate and protect children online, but also because such behaviours have been shown to be indicative of later behaviours and attitudes [40, 41, 78]. To this end, we build on recent work examining children's perceptions of online privacy risks [26, 41, 53, 83], and extend existing literature in two ways: first, by examining in detail how children *describe* certain common kinds of risks, for the purpose of understanding their conceptualisations of them; second, we examine the risk coping strategies taken by the children for each distinct risk context. Specifically, we focus on the following three research questions:

- *R1: Perception* - Do children care about privacy online? When they do, how do they describe privacy risks?
- *R2: Recognition* - How do children recognise risks? What information do they use in the process?
- *R3: Response* - How do children apply their existing knowledge in responding to risks in different scenarios, including threats they never experienced before? What do such responses suggest about information and knowledge that might be needed?

We report our results based on 12 focus groups with 29 children, aged 6-10, from UK schools undertaken between June and August 2018. We found that children in our study had a good understanding of risks related to *inappropriate content, the approach of strangers*, and *oversharing of personal information online*. However, they struggled to fully understand and describe risks related to *online game/video promotions and personal data tracking*. Moreover, children's risk coping strategies depended on their understanding of the risks and their previous experiences: effective risk strategies were applied only if children recognised certain risks or when they *felt* something untoward. These findings demonstrate the importance of learning about potential risks through a multitude of channels, such as school, parents, friends, siblings, and personal experiences [34, 81].

We identified significant gaps in children's current awareness and understanding of two major forms of online risk: (i) online recommendations, and (ii) implications of data tracking, i.e., the recording and sharing of data pertaining to what they do online. Children remain poorly equipped to identify targeted promotional material online, including adverts and in-app promotions, exploiting tracked activity data. We offer recommendations on the development of tools to facilitate children's understanding of privacy risks, and the need to extend children's awareness of implicit personal data access, which is becoming ever more prevalent in the games and content they encounter [13, 20, 65].

2 BACKGROUND

Children's Perception of Privacy

Privacy has been described as a "concept in disarray"[69] reflecting the complex and often overlapping conceptualisations. O'Hara proposed "seven veils" of privacy, spanning the conceptual, factual, phenomenological, preferential, societal, legal, and moral [61]. Practical research in privacy has typically spanned multiple such veils; Livingstone suggests that privacy is related to the keeping of information out of the public domain or the effective determination of *what* personal information is made available to *whom* [44]. Nissenbaum's theory of Contextual Integrity (CI) frames privacy as "the right to appropriate flow of personal information" [59] where what is "appropriate" is based on particular contexts and relationships. CI has been found to be a useful practical framework to interpret people's perceptions of privacy [10, 43].

Managing privacy is becoming increasingly challenging, given the vast (and growing) information asymmetries of the digital age [7], where data about people are harvested by powerful platforms and vast networks in ways they do not understand nor recognise. Children are particularly susceptible in part due to them having little sense of the risks posed by the accumulation of personal data over time [62]. The combination of such a lack of understanding, with incentives put in place by apps and platforms to get people to share their data, have yielded the so-called 'privacy paradox', a behaviour studied in teenagers [14] and adults [11] alike, in which individuals act in ways contrary to their stated privacy preferences and concerns [37, 38, 62]. Recent studies showed that although teenagers from 14 to 18 were typically concerned about being personally identified by their personal data, they failed to perceive the potential threat of re-identification via the particular fragments they shared, e.g., images or geo-location [62].

Whilst there has been extensive research on teenagers' perceptions of privacy, relatively little has been done for children aged below 11. They have often been perceived as being too young to understand privacy or exercise digital independence online [47]. However, developmental research has shown that children can develop a "theory of mind" by the age of 4 [19], which enables children to recognise the differences between concepts in their minds and those in others, and hence to grasp complicated concepts like "secrecy" [19] or "deception" [17]. Contrary to common expectations, children value their privacy because this enables them to enjoy their experience online [41, 68], such as socialising with their friends and families or experimenting with new games.

Recent research with 14 Canadian families showed that children aged 7-11 can align online privacy with real-world scenarios such as "being left alone" or "hiding secrets", and draw an analogy to the online environment through expressions like "keeping things to yourself" or "not talking to strangers" [83]. Kumar et al. [41] unpacked the perception of online privacy for 26 US young children and examined how they were able to recognise sensitive entities (such as passwords) but struggled with identifying risky actors (strangers) involved in questionable contexts. These studies provide useful insights into children's perception of risks, i.e. what they think of as being risky, and what they struggle to recognise; however, they do not tell us how children make these judgements - or whether children can in fact identify a threat and its origination.

Managing Children's Privacy Online

Tools developed for managing children's privacy on mobile platforms usually comprise features that monitor and restrict children's online activities [46, 60, 77]. Children often find these tools overly restrictive and invasive of their personal privacy [30, 77]. Co-design studies with children under 12 show that they prefer technologies that facilitate their risk coping skill development, promote communication and interaction with their parents, and emphasise restrictions around monitoring [53]. However, such tools are still scarce.

Several recent studies have recognised the importance of supporting children's learning through approaches like interactive storytelling [82], game playing [52] or co-learning with parents [34]. They have shown the effectiveness of increasing children's awareness of related online safety issues, such as online personal identity or content appropriateness. This demonstrates that a knowledge scaffolding approach to a child's means of dealing with privacy risk coping could provide a useful addition to safeguarding their cybersafety.

Developmental Stages of Privacy Concepts

Children's ability to recognise privacy risks may be intrinsically limited by their developmental stage. At ages 3 to 5 years, children start to build up friendships; however, at this stage, family interactions are dominant, and many of their online activities are still parent-guided [40]. At this stage, peer pressure is less of an influence [9]. Children from 6 to 9, however, start to learn about the complexity of relationships and feel the need to fit in to peer social groups [9]. They are also more involved in online activities and enjoy playing games with their friends [40]. This social interaction with peers makes them more aware of interpersonal privacy risks, but less of other privacy risks [40]. So while they often care deeply about their personal information being shared with their peers, parents, and others online, they remain unaware of other actors, including platforms, app designers, malicious actors, and others operating in digital ecosystems [50, 62].

Vygotsky's Zone of Proximal Development (ZPD) is a theory that relates the difference between what learners can do independently to what can be achieved by through guidance by a skilled partner [16]. It has been applied to assess the effectiveness of teaching and learning [55], to identify key barriers in learning by understanding knowledge gaps [22], and in the design of better intelligent tutoring systems (ITS) [64]. Inspired by ZPD, we focus on identifying children's misconceptions of privacy risks and highlighting areas of knowledge that could be developed through future active scaffolding.

3 STUDY DESIGN

Given our focus on understanding children's ability to recognise privacy-related contexts by examining how they describe them, we chose the focus group method to elicit children's responses to a collection of hypothetical scenarios that reflect different types of explicit and implicit threats to children's online personal data privacy.

Focus Groups with Children

The role of children in research is increasingly recognised, as children are key stakeholders in modern digital technologies [23]. Focus groups put children at the centre of the research, and encourage the sharing of their perspectives and experiences [31, 32, 57]. They are often used to facilitate group dialogues around the topic of interest and result in findings that cannot be obtained through individual interviews [70]. Focus groups have been successfully used to study children's experiences in different fields, such as health sciences (e.g. studying children's experience of living with asthma [57]), in sociology (e.g. studying children's experiences with bullying [33, 56]), or in understanding children's experiences with technology [24, 26, 27].

These previous studies have demonstrated that using focus groups with children can reduce the influence of adults, and encourage children to keep each other on track and truthful. However, conducting focus groups can be challenging, given the power dynamics amongst the children and the different forms of expression preferred by different children. Based on the experiences of several previous focus groups with children under 11 [26, 57], we took the following decisions in our study design: 1) keeping children from the same age group together; 2) using role playing to relax children and balance the power between the adult and children; and 3) providing options for children to express themselves using other methods like pen and paper.

Scenarios

In our focus group discussions, we chose to walk through a series of hypothetical scenarios with participant children, about a cartoon character named Bertie, an 8-year-old koala bear who likes playing with tablets, but is not always certain how to cope with unusual events taking place during his use of the mobile apps (see Figure 1). Hypothetical scenarios are effective ways of collecting children's perception of online security and privacy [41], by making them feel they are not being judged [73, 79].

Our scenarios were carefully designed to contrast explicit versus implicit data collection in a familiar versus unfamiliar technology context. Previous research has shown that children under 11 particularly struggle to understand risks posed by technologies or comprehend the context of being online [41, 83]. They have explored how children responded to *explicit* data requests such as in-app pop-ups; while our study also looks into children's awareness and perception of *implicit* data access through third-party tracking, which leads to personalised online promotions.

Story 1 — Implicit video promotions are widely found in applications like social video sharing platforms, which can be based on personal viewing history or a viewers' interests. Online promotions on such platforms are a significant means by which children discover games or video channels, material that is not always appropriate for their age or developmental needs [48]. Therefore, story 1 aimed to assess how much children are aware of the video promotion behaviours of online platforms, some of which could be based on children's online activities, including the videos they have watched or the games they enjoy playing.

Story 2 — In-app pop-ups can explicitly prompt children for personal information (such as names, age or voices) before they can continue with the game. Story 2 aimed to assess children's awareness of *explicit* stranger danger and in-app game promotions, which can be personalised based on their online data.

Story 3 — The large number of applications ('apps') that can be downloaded for free are a major way by which children interact with these devices. Currently these 'free' apps are largely supported by monetisation of user's personal information [8, 43]. A large amount of personal information and online behaviour may be collected from children's apps and shared with third party online marketing and advertising entities [65]. This scenario is designed to examine how children perceive and feel about these risks.

Scenario 1 and 3 are closely related to children's ability to comprehend the impacts of data-driven decision-making, i.e. their 'big data' literacy [25]. Previous research has shown that children aged 8-16 were capable of critiquing analytics applied to the data about them [35] and recognise issues related to algorithmic accuracy and fairness. Our study complements previous research by looking into how much children aged 6-10 are aware of the context in which their personal data may be collected, transmitted to other online actors, and then used to drive algorithm-based decision-makings.

4 STUDY METHOD

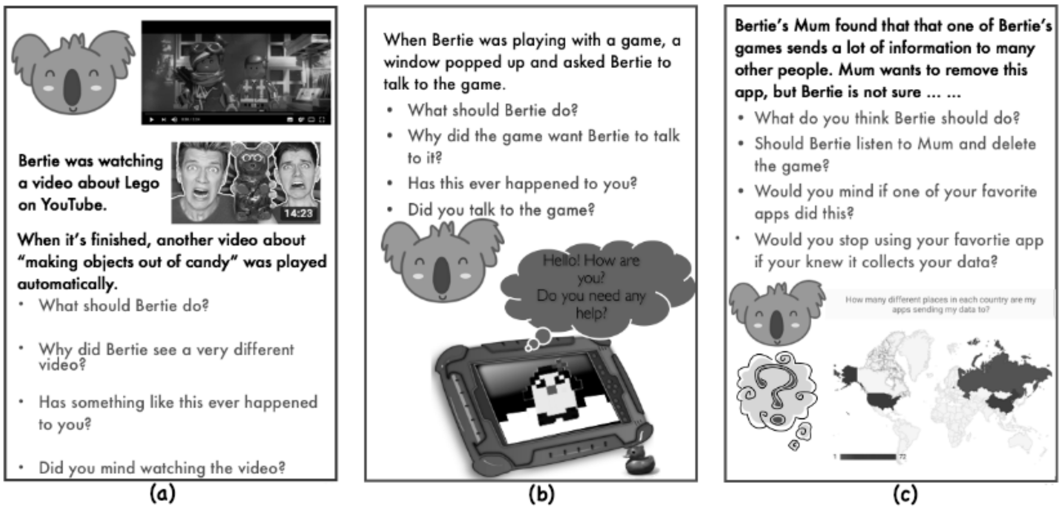
Participants were recruited from both local primary schools and a public forum for advertising local family events. Recruitment started in May 2018 after obtaining ethics approval, and 12 studies were carried out between June and August 2018. Half of the studies took place on school premises during school term time, and the other half in our university premises during the summer holiday period. At school, a school teacher or teaching assistant was present in the room, at the university, parents left the children in the room and waited outside until the study was completed. The majority of the participants were recruited through schools and school newsletters. Each study was facilitated by one researcher along with two note-takers.

Study Process

Each focus group study contained four parts, including a warm-up and introduction session, a sharing of favourite apps, a walk-through of the hypothetical risk scenarios, and finally an open-ended session about issues not so far discussed. The whole study was planned to last around 1 hour and each part of the study was designed to be fun and framed as a game. We avoided using words like 'dangerous' or 'suspicious' in our scenarios.

The warm-up session included a game of "throwing a ball" [57] and invited everyone in the room to share their favourite colour and food with the others. The session normally lasted 10 minutes. It helped participants, particularly young children, to relax. Then we used an iPad to ask children to show us their favourite apps, or search for them in the app store if they could not find them on our device. Children were then asked to comment on why they liked the app. This gave us insight about what children in our study enjoyed doing online and their positive experiences.

During the session discussing the three hypothetical scenarios, we let everyone choose a soft toy in the room and role played a character each, such as Bertie's sibling, parent or teacher, in order to help participants (particularly quiet



Bertie was watching a video about Lego on YouTube.

When it's finished, another video about "making objects out of candy" was played automatically.

- What should Bertie do?
- Why did Bertie see a very different video?
- Has something like this ever happened to you?
- Did you mind watching the video?

When Bertie was playing with a game, a window popped up and asked Bertie to talk to the game.

- What should Bertie do?
- Why did the game want Bertie to talk to it?
- Has this ever happened to you?
- Did you talk to the game?

Bertie's Mum found that that one of Bertie's games sends a lot of information to many other people. Mum wants to remove this app, but Bertie is not sure ... ...

- What do you think Bertie should do?
- Should Bertie listen to Mum and delete the game?
- Would you mind if one of your favorite apps did this?
- Would you stop using your favortie app if your knew it collects your data?

14:23
Hello! How are you?
Do you need any help?
How many different places in each country are my apps sending my data to?
1
72
(a)
(b)
(c)

Figure 1: Three hypothetical scenarios for focus group discussion (original story cards were in colour): (a) shows a video promotion scenario; (b) illustrates an in-app pop-up requesting children's inputs; and (c) depicts how children's personal data could be tracked and sent to third parties without their knowledge or explicit consent.

children) feel they are not being judged [57]. In each hypothetical scenario, children were first given some time to read through the printed story cards (as illustrated in Figure 1). If they had trouble, one of the note-takers would provide help and read along with them[1]. While children were first asked to respond to the predefined questions, like *what will you do* or *what do you think Bertie should do*, our facilitator followed up any responses that required further clarifications (such as what do you mean by "hacking"). This session also encouraged children to share their personal experience related to the scenarios, by asking questions like *whether this has happened to them* and *what you did*. This enabled us to listen to children's descriptions of their experiences not covered in the scenarios.

Audio and video recordings were taken during the studies; two note-takers provided additional details about key interactions they observed. Video recordings were played back during the transcription and data analysis phases to highlight any notable interaction patterns between participants.

Participant Information

We had 29 participant children, including 14 boys and 15 girls, with an average age of 8.5 (range = 6-10, s.d. = 1.4). Details about participants can be found in Table 1. In total we had 12 focus group and the group size varied between 2 and 4 [29], with an average group size of 2.4.

Children in our study were generally more attracted to 'fun' games that they found exciting or could learn new things from. They were also influenced by friends and families on the choice of apps ('so that I can play with friends'). 25/29 children owned their tablets or phones, while the rest used their parents' devices or shared with their siblings. Online promotions (e.g in-app promotions, app store adverts, YouTube videos) had influenced many children's choice of apps; 20/29 children reported that they have seen promotions in their games or videos, and 12 children reported that they found their favourites or installed new games through these means.

Age	#Boys	#Girls	#Total
6-yo	4	0	4
7-yo	1	0	1
8-yo	3	3	6
9-yo	3	4	7
10-yo	3	8	11

Table 1: Summary of participants' ages and genders

5 DATA ANALYSIS METHOD

We transcribed the interviews and analysed the data in two iterations. In the first iteration, we used a thematic analysis method to develop codes and themes related to risks talked about by the children and how they coped with them.

The thematic coding process started by dividing the transcriptions into two (roughly) equal-sized sets. The first three authors independently analysed the first set of transcriptions to derive an initial set of codes. Then they met to consolidate and reconcile codes into a common codebook. These codes

[1] Reading literacy is widely promoted in the U.K. for children aged 4 years and above. The story cards were written in as simple a language as possible and were tested with children aged 6yo.

were then applied to the second (yet unseen) set of transcriptions by the same set of researchers, and Fleiss' kappa [28] (0.83) was computed to assess inter-coder reliability.

In the second iteration, we used the CI framework, particularly its four-parameter model, to examine the risks identified by the children (either from our hypothetical scenarios or their own experiences with technologies) and how they were described by the children. The four parameters from the CI framework include the following:

- *Attributes*: the types of information being transmitted, such as users' data, personal information, etc.
- *Contexts*: the situation or scenario to which the social norms may be applied.
- *Actors*: the entities involved in the information transmission, which can be the subject, sender or recipient of the information.
- *Transmission principles*: the way information is transmitted from the sender of information to the recipients.

This four-parameter model helped us to calibrate whether children recognised the exact actors, attributes, context and information transmissions involved in each risk context, led us to delineate three categories of risk recognition by children, namely *accurate, vague and missed* risk recognition.

6 RESULTS

We present our results by first outlining children's use of language under each category of risk recognition (i.e. recognised, vaguely or missed). We then present an overview of children's responses to the three hypothetical scenarios, before providing in-depth analysis regarding children's risk coping strategies when risks were recognised, vaguely understood or missed. In this way, we demonstrate an understanding of children's current knowledge gaps in describing and coping with risks.

Children's Use of Language Under Each Category of Risk Recognition

We observed that some terms were repeatedly used by children across different situations. Moreover, as shown by the examples in Table 2, children were able to describe risks accurately when they could recognise the actual risks. However, when they had only a vague understanding of the risks, they struggled to describe things consistently or to provide a good explanation of what they meant.

Good risk recognition and accurate description

When children recognised the actual risks, such as inappropriate content or over-sharing of personal information, they could describe them quite accurately, for example, using terms like *'personal information'* or *'private information'* to refer to the type of information they treated as sensitive; or words like *'things for adults'* or *'not my age'* to refer to content that was inappropriate to them.

Vague risk recognition and inconsistent descriptions

When children only made a partial sense of certain types of risks, their use of terms can be inconsistent. For example, although some children were able to describe the scenario of new videos being presented to Bertie using words like 'people trying to make money' or 'them trying to make you watch more', they struggled to explain who these 'people' are and how information might be transmitted to these '[YouTube] channel people' in this context. Another example is the term 'hacking', which has been used by children across different focus groups, but in fact with very different meanings. For example, when trying to explain why a new video was shown following a previous video, children used 'hacking' to mean 'someone stole my data', 'take your account', or 'steal from house'. 'Hacking' has been used by the same group of children to make sense of other scenarios, including in-app pop-ups or data tracking.

Feelings and experiences, but no recognition of risks

When children could not describe the exact risks they encountered, they would refer to a feeling of 'scary' or 'annoying' to talk about times when they felt a need to take an action. Children also referred to things they 'had experienced before' when they could not describe why something made them take actions. This indicates that although sometimes children probably did not fully comprehend their previous experiences, the consequences provided a signpost for them to stop [37].

Children's Responses to the Hypothetical Scenarios

Table 3 summarises how children responded to our three hypothetical scenarios:

- In the video-related scenario of story 1, which aimed to assess children's awareness of (personalised) game promotions, children largely *missed* these risks and associated this context with 'autoplay' or computers trying to 'save your time'; only three groups associated this context with YouTubers trying to 'make money'. 9 out of 12 groups suggested that they would 'play and see', and half of the groups suggested that Bertie should tell his parents. However, when asked what they would do in this scenario, all but one of the groups would play the video and make a judgment by themselves, instead of seeking advice from their parents.
- Story 2 aimed to assess children's awareness of stranger danger and in-app game promotions, which again can be personalised. Apart from one group, all children agreed that *pop-ups should be treated with caution*, whilst they made different interpretations of pop-ups,

Context	Risks	Words	Children's explanation of the meanings
Risks recognised	Inappropriate content	*weird things*	*things for adult, not my age*
	Threats from strangers	*strangers,*	*random people, or I don't know*
	Person information over-sharing	*personal information*	*everything about me, my stuff, personal photos*
Risks vaguely understood	Online promotions	*Channel people, app developers*	*I don't know*
		get more subscribers	*more money and more famous*
	Pop-ups	*hacking*	*steal from house, take your account, steal your data*
	Data tracking	*hacking*	*track your personal information*
		tracking	*try and find you, find your location, know more about what's happening in this country*
No risks specified		*scary, angry, upset, annoying, surprised*	

Table 2: Example descriptions of risks felt, experienced, recognised or interpreted by children.

Context	Bertie should?	You would?	Why?
Story 1	Play-and-see, or tell parents	Play-and-see, or continue (because it is fun)	*autoplay, making it easier (to watch), based on past history, people making money*
Story 2	Stop, delete, or tell parents	Shut off or delete	*hack you, trick you, steal the voice, access personal information*
Story 3	Stop, tell parents, or do some research	Stop	*my information, depending the companies*

Table 3: Children's responses to hypothetical scenarios — what to do and why

which could be 'hacking' (i.e. 'stealing their information or voice data') or 'tricking them to buy things'. Even though the perception of risks differed, all children suggested that both Bertie and they should go and tell someone about this, or immediately delete or stop using the app.

- For story 3, which focused on the tracking behaviour of apps, an aspect still largely unfamiliar to adults and children alike, 'telling parents' and 'discussing with parents' were suggested by 10/12 groups as the coping strategies, even though children didn't fully understand who might access this tracked data. A few older children (9-10 yo) also suggested that they would do some further research with their parents to figure out what kind of information might be collected or who the companies might be that were receiving this information. All children said that Bertie should stop using the app and they would stop using their favourite apps too.

Risk Coping When Risks Were Accurately Recognised

Children demonstrated a strong consciousness of their online identity and the importance of avoiding sharing their real identity or over-sharing their personal information. In these cases, children applied various effective strategies to protect their sensitive personal information. For example, a 10-yo girl demonstrated her knowledge of using an obfuscation strategy to protect her real identity online:

> 'I make up a name cause I don't want people know my name' – C6, a 10-yo girl

Others mentioned techniques they would use to verify the identity of anyone who tried to contact them online:

> 'If I know who they are and they told me their names and accounts, and if they ask me in person to friend them, then I would friend them. If I don't know who they are and haven't seen them in real life then I wouldn't accept them' – C14, a 9-yo girl

These risk coping strategies are effectively applied by the children when they face explicit inappropriate content or an explicit request for their personal information from platforms or apps. However, our analysis showed that children may struggle to fully understand risks in other contexts. In the following sections, we unpack how children responded to situations when they struggled to recognise or understand the risks fully, summarised in Table 4.

Risk Coping When Risks Were Vaguely Understood

In contrast to explicit privacy risks, children struggled to associated online promotions with losing control of personal information. The effectiveness of their risk coping may vary — they may be cautious even though not fully understanding risks, or open to try-it-and-see strategies.

Open to Recommendations

Several children discussed their interpretation of how YouTubers may try to 'persuade' them to watch their videos in order to gain 'money' or 'more subscribers'. For example, a group of 8-yos shared their knowledge about how the number of subscribers to an online video could be related to the reward to the video publisher.

> 'C12: eurgh, they get money and they get more famous
> C10: if you watch their video a lot, then they get a lot of thumbs ups of their videos
> C13: they have lots of subscribers'

However, none of these children expressed resistance to these video promotions. They treated it as if this is how the Internet works – 'if they reach the max subscribers, then they get the money' (C12). Their primary decision making

Context	Descriptions and examples	Children's risk coping strategies
Risks recognised	inappropriate content request for sensitive personal information approaching by strangers	*ask for help* *stop* *avoid oversharing*
Risks vaguely understood	Online promotions == recommendations	*it's ok, let's play*
	Tracking == hacking	*stop* *ask for help*
	Pop-ups == hacking	*stop* *ask for help*
Risks missed	New videos == auto play	*it's ok, let's play*
	Familiar YouTuber/games == Ok	*it's ok, let's play*
	I/My friends played it before == Ok	*it's ok, let's play*

Table 4: Children's Risk Coping Strategies Depending on Their Ability to Recognise Risk Contexts

was still based on whether the content was interesting or whether it was from their favourite video providers.

Play-and-See When Not Fully Recognising Recommendations

Only a few children (3/12 focus groups) recognised how new videos might be related to personalised recommendations. One group of 10-yo children used the word 'recommendation' to describe video promotions on YouTube. However, they struggled to understand *who* was performing these recommendations, and as a result, they were less sure about the consequences for their privacy.

> 'C2: because it recommended this.
> C1: maybe he watched other videos like that. and then this one popped up
> R: how did you know about that?
> C1: not sure'

As a result, the children usually applied the play-and-see strategy to assess the content or apps they came across, without any more complex reasoning.

Stop, Even Not Fully Recognising What Hacking Involves

Children associated a diverse range of scenarios with the word 'hacking'. Sometimes it was used deliberately to refer to actions (or intentions) by app and platform designers, rather than activities of computer criminals. For example, the following description from a 10-yo girl referred to her experience with location tracking by Snapchat. She understood risks associated with location tracking, even though she used the word 'hacking' to describe tracking behaviour of the app:

> 'Yeah, that's why I put on ghost mode, so they can't find your location. So yeah, they try to hack your tablet and they can get all the games you like to play in, all the personal information, like what school you go to' – C5, a 10-yo girl

Other times, children might use the word to refer to being personally coerced or made to take an action by an app or service. For example, C24 (a 7-yo girl) tried to explain why she thought Bertie should not watch the new video by saying that

> 'It is a bit random and just pops up ... someone might be trying to hack you or something'. – C24, a 7-yo girl

In such a situation, the concept was 'hacking' was used to provide a possible explanation as to *why* or *by whom* they were being made to take particular actions–which they struggled to fully understand.

This was particularly common among younger children under 8 (11/29), who could not explain what they meant by 'hacking' when this word was used in their interviews. In these situations, because children recognised that 'hacking' is a bad thing, they would take effective action to either stop or ask for help from parents, even though their actual recognition of the risks were vague or misinformed.

Risk Coping When Risks Were Missed

Children could miss risks due to a lack of knowledge, or due to their past experiences, which did not lead to any direct consequences related to the risks. For those children who interacted with certain technologies and experienced no implications before, they would tend to be more (over-) confident with technologies.

Associating New Videos with 'Autoplay'

Children from 7 focus groups treated online video promotions as part of an 'autoplay' function of the platform, without questioning how the new content might be presented to them. 12/29 children demonstrated trust in the content provided by their familiar YouTubers. For example, C4 (a 10-yo girl) mentioned that 'because it's one of my favourite YouTubers. So I was ok with it'.

As a result, children reported having been exposed to unexpected content and online baiting. These same children reported that they often saw upsetting content online (e.g. 'sometimes in autoplay, it comes up with these really freaky ones like pictures of dead people ' — C5, a 10-yo girl). 12 (out of 29) children in our study reported how their favourite games were discovered through promotions in the videos they watched ('A friend and I were watching YouTube and we saw people playing this game.' – C14, a 8-yo girl).

Familiarity Overwrites Rules

Our data also shows that familiarity could give children a fake sense of safety. For example, C3 (a 10-yo girl) mentioned that 'I don't think YouTube and stuff like that could collect much', and another two 10-yo girls discussed how their experiences with a known app had a strong influence on their judgement upon whether an app could pose threats to them or not.

> 'C8: It depends on what game it is. If it's like the talking Tom, then that's fine because you're safe.
> C9: Yes, cause it doesn't record you and keeps it.
> C8:Because I play it all the time and nothing has happened to me and I'm always talking to it. I haven't had any problem with my ipad
> c9: Yes me too, I've been playing with it for one to two years and haven't had any problem.'

Experience-Centric Decision Making

We also observed that a child's or their peers' personal experiences had a strong influence upon their decision making, even though they didn't always understand what may pose threats to them. The following example illustrates how children in our study demonstrated that they used experiences as a heuristics for their decision making, as described by C27, a 10-yo girl, 'If my friends already play it I wouldn't bother checking it cause they know it's safe. If it's one I didn't know about then I wouldn't use the app'.

7 DISCUSSIONS

Key Findings and Contributions

Our results reinforce existing findings that children under 11 struggle to fully understand online privacy risks [15, 26, 40, 41, 83], especially those associated with implicit personal data collection and use, through mechanisms such as data tracking or in-app recommendations. However, our results also demonstrate that children cared about, and were sensitive to, who might access their sensitive information (e.g. real names, age, location etc), and applied a range of techniques to safeguard this space, such as by verifying identities through face-to-face interactions or avoiding using real names as usernames. Children felt 'annoyed', 'surprised' or 'angry' when they felt coerced, or felt not in control. Our results also reinforced that, like teenagers and younger children, our participants valued the positive experiences of being online and keeping in touch with their friends, and their personal space online [51].

Implications for Designing for Children

It is clear that current digital technologies are often not designed with children's best interests in mind. For example, social media platforms widely used by children (such as Instagram or Twitter) keep their profile pages as public by default[5], and games from the 'family' genre from the leading mobile app markets are associated with more third-party trackers than games designed for adults [13, 66]. For younger children, smart toys and connected baby monitors can continuously stream video and audio information to data centres in ways that are completely opaque to children and/or parents [54].

Although the need to provide a better design for children is recognised by the recent development of regulations (such as the General Data Protection Regulation (GDPR) [3]) and proposals for age-appropriate design for children [2], children are only occasionally consulted in these efforts [4]. Designers, as well as policymakers, should recognise children's interests as well as the need to involve children [42, 53] in the process of design and policymaking.

Implications for Privacy Tools Supporting Parents and Children

Our findings confirmed children's ability to recognise certain privacy risks. But we need to expand children's understanding of implicit data collection risks. Current tools for safeguarding children online mainly focus on enabling parents to take control or monitor children's online activities [41, 77]. Related research with parents and their teenagers have shown that current tools often work against parents' and children's values of privacy, and they would prefer tools to facilitate parental mediation of children's use of technologies rather than simply providing surveillance capabilities [76, 77]. Parental involvement leading to improved learning outcomes of children is extensively supported by existing literature [18, 74]; however, parents feel they are poorly supported in dealing with challenges related to facilitating their children's use of digital technologies [46]. Most of the time they rely on self-guided online searches, rather than being informed by systematic, comprehensive and reliable resources [46]. Future tool development should consider both scaffolding children's knowledge acquisition and facilitating the active involvement of the parents.

Several studies have looked into how to facilitate children's learning of online privacy and safety through a co-learning process between parents and children [34, 81], and demonstrated their effectiveness for increasing children's risk recognition and coping. However, the difficulty of recognising data tracking risks is not unique to children, suggesting the need for better tools to help provide some transparency to adults and children alike [7, 72]. Greater transparency could also support children's ability to make sense of the personalisation and recommendation behaviours of online platforms that dominate our information consumption online [25], by providing information about why or by whom particular content was recommended. However, given children's development stages, especially those under 11, they probably have less ability to fully recognise the implications of these risks. Therefore, tools designers should not only help parents mediate children's understanding of online risks but also help them to develop "big data" literacy [35] to start to understand how information derived from online activities are captured, retained and repurposed by various entities, as well as the potential risks such retention, processing, and use carry.

Reflection on Methods

Focus groups have been instrumental in our understanding of children's perception of risks and their way of describing these risks. This approach has provided an open setting to incentivise children's sharing of their experiences, and particularly those of their peers, like friends or siblings. In comparison to previous studies [41, 83], in which semi-structured interviews with parents and children were the main method used, our focus group studies with children inspired more discussions about children's and their peers' experiences with online privacy risks. These have been a principal means for us to have a deeper understanding of how children's risk coping strategies may vary under different contexts.

The CI framework provides a useful philosophical framework for understanding the social and ethical aspects of privacy. However, translating it into a technical implementation is not straightforward [12]. Most of the previous work has used *context* as a synonym for a scenario or situation, to understand users' privacy preferences and expectations [75, 80]. Others have used the concept to design social platforms that can adapt to different social norms in different spheres (like families, friends, colleagues etc) [21, 71].

Kumar et al. [42] have applied the normative aspect of the CI framework to assessing how well children can recognise the *actors, information entities and information transformations* involved in a context. This work extends and builds on their findings: by examining children's privacy mental models, we focused on the terms used by the children for describing privacy contexts and related factors (e.g. the information that is sensitive to them or the organisations that are regarded as threatening). We look for a deeper understanding of both the types of risks that children struggled to recognise (such as third-party tracking) and to describe these accurately. This has been an effective process to understand children's current knowledge gaps and the key information that is needed to facilitate their future development of privacy knowledge.

8 LIMITATIONS AND FUTURE WORK

We acknowledge that it is difficult to generalise our findings given the sample size and study population. First, schools and parents who chose to participate in the study may already be more interested in the topic than the average population. This may have impacted the *a priori* awareness of online privacy risks our participants had. Secondly, whilst we did not collect information about participants' family income, the families' areas of residences were centred in an affluent area near a university. This may have resulted in our findings reflecting a greater privacy literacy than the general population, not only due to familial influences, but also due to local schools. Our primary goal, however, was not to measure the degree of literacy or concern, but the gaps of greatest concern and potential for new tools to help. While we did not explicitly look at age-specific differences, informally we noticed possible differences we wish to examine further in future work; e.g. children older than eight seemingly demonstrating a richer vocabulary to describe risks. Finally, when the focus group studies were carried out at schools, a teaching assistant or a class teacher was often present in the room, for safeguarding reasons. Children may have moderated their responses in these settings.

Future work also aims to explore how we may design approaches that could enable children to expand their knowledge about online privacy risks in two ways: new knowledge scaffolding based upon children's actual understanding, and addressing the critical knowledge gap about online promotions and data tracking. Our study emphasises the importance of scaffolding children's understanding of risks and privacy strategies. Given children's role in these digital technologies, we intend to use co-design workshops [42, 53], involving children, parents, teachers, and designers of educational games, to explore approaches to scaffolding children's privacy knowledge.

9 CONCLUSION

Inspired by the ZPD theory and the Contextual Integrity framework, our work examined children's current knowledge about privacy risks online and how children may or may not have fully recognised online privacy risks when adopting particular strategies. Our results showed that children's ability to fully recognise privacy risks has a direct impact on their ability to consistently describe and manage these risks: when they only vaguely recognised the risks, they would try to make sense out of them using their knowledge or experiences, but would not always take effective action. Expanding our understanding of children's perceptions of risks thus advances the goal of facilitating a child's ability to cope with risks from a young age, scaffolding this through a knowledge acquisition, rather than a restrictive approach. We hope that our findings will support both designers of new privacy tools for children, as well as those of educational material seeking to address gaps in their understanding of risks and data use online.

Providing better privacy-by-design guidelines for protecting children is essential both to influence, and meet the aspirational goals of data protection (DP) initiatives being set forth around the globe. Although the GDPR in the EU protects the use of children's data, the Children's Online Privacy Protection Act (COPPA) in the US has yet to provide an explicit regulation of third-party tracking. This study has highlighted some potential avenues by which future tools might, through greater data literacy, lay the foundation for having children understand, and start to exercise, the rights such DP regulation grant them.

10 ACKNOWLEDGMENTS

We thank participant schools and children for their time, and the anonymous reviewers for their feedback. This work was supported by the EPSRC Impact Acceleration Account KOALA (EP/R511742/1).

REFERENCES

[1] 2013. *Zero to Eight: Children's Media Use in America 2013.* Technical Report. Common Sense Media. https://www.commonsensemedia.org/research/zero-to-eight-childrens-media-use-in-america-2013

[2] 2018. Call for evidence - Age Appropriate Design Code. https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-evidence-age-appropriate-design-code/. Accessed: 2018-09.

[3] 2018. Children and the GDPR. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/. Accessed: 2018-08.

[4] 2018. Children's rights and the GDPR – are the new consultations creating light or further confusion? http://blogs.lse.ac.uk/mediapolicyproject/2017/05/11/childrens-rights-and-the-gdpr-are-the-new-consultations-creating-light-or-further-confusion/. Accessed: 2018-08.

[5] 2018. Instagram Help Center. https://help.instagram.com/116024195217477. Accessed: 2018-08.

[6] 2019. Must Have Apps for Kids Under Five. https://www.lifewire.com/great-apps-for-kids-5-and-under-4152990. Accessed: 2019-02.

[7] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[8] Alessandro Acquisti, Curtis R Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of Economic Literature* 52, 2 (2016).

[9] Birch Ann. 2000. The Developmental Psychology-from infancy to adulthood. *Bucharest: The Technical Publishing House* (2000).

[10] Louise Barkhuus. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 367–376.

[11] Susanne Barth and Menno DT De Jong. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038–1058.

[12] Sebastian Benthall, Seda Gürses, Helen Nissenbaum, Cornell Tech, and NYU Steinhardt MCC. 2017. Contextual Integrity through the Lens of Computer Science. *Foundations and Trends in Privacy and Security* 2 (2017), 1–69.

[13] Reuben Binns, Ulrik Lyngs, Max van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt. 2018. Third party tracking in the mobile ecosystem. *Proceedings of the 10th International ACM Web Science Conference 2018* (2018).

[14] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347.

[15] Tanya Byron. 2010. Do we have safer children in a digital world? A review of progress since the 2008 Byron Review. (2010).

[16] Seth Chaiklin. 2003. The zone of proximal development in Vygotsky's analysis of learning and instruction. *Vygotsky's educational theory in cultural context* 1 (2003), 39–64.

[17] Michael Chandler, Anna S Fritz, and Suzanne Hala. 1989. Small-scale deceit: Deception as a marker of two-, three-, and four-year-olds' early theories of mind. *Child development* (1989), 1263–1277.

[18] Cecilia Sin-Sze Cheung and Eva M Pomerantz. 2011. Parents' involvement in children's learning in the United States and China: Implications for children's academic and emotional adjustment. *Child development* 82, 3 (2011), 932–950.

[19] Malinda J Colwell, Kimberly Corson, Anuradha Sastry, and Holly Wright. 2016. Secret keepers: children's theory of mind and their conception of secrecy. *Early Child Development and Care* 186, 3 (2016), 369–381.

[20] Federal Trade Commission et al. 2015. Kids' Apps Disclosures Revisited.

[21] Natalia Criado and Jose M Such. 2015. Implicit contextual integrity in online social networks. *Information Sciences* 325 (2015), 48–69.

[22] Harry Daniels. 2005. *An introduction to Vygotsky*. Psychology Press.

[23] Allison Druin. 1999. *The Role of Children in the Design Technology*. Technical Report.

[24] Jill Dunn, Colette Gray, Pamela Moffett, and Denise Mitchell. 2018. 'It's more funner than doing work': children's perspectives on using tablet computers in the early years of school. *Early Child Development and Care* 188, 6 (2018), 819–831.

[25] Catherine D'Ignazio and Rahul Bhargava. 2015. Approaches to building big data literacy. In *Proceedings of the Bloomberg Data for Good Exchange Conference*.

[26] Lesley-Anne Ey and C Glenn Cupit. 2011. Exploring young children's understanding of risks associated with Internet usage and their concepts of management strategies. *Journal of Early Childhood Research* 9, 1 (2011), 53–65.

[27] Jennifer Fane, Colin MacDougall, Jessie Jovanovic, Gerry Redmond, and Lisa Gibbs. 2018. Exploring the use of emoji as a visual research method for eliciting young children's voices in childhood research. *Early Child Development and Care* 188, 3 (2018), 359–374.

[28] Joseph L Fleiss. 1971. Measuring nominal scale agreement among many raters. *Psychological bulletin* 76, 5 (1971), 378.

[29] Melissa Freeman and Sandra Mathison. 2008. *Researching children's experiences*. The Guilford Press.

[30] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say About Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing*

Systems (CHI '18). ACM, New York, NY, USA, Article 124, 14 pages. https://doi.org/10.1145/3173574.3173698

[31] Faith Gibson. 2007. Conducting focus groups with children and young people: strategies for success. *Journal of research in nursing* 12, 5 (2007), 473–483.

[32] Sheila Greene and Diane Hogan. 2005. *Researching children's experience: Approaches and methods.* Sage.

[33] Nancy G Guerra, Kirk R Williams, and Shelly Sadek. 2011. Understanding bullying and victimization during childhood and adolescence: A mixed methods study. *Child development* 82, 1 (2011), 295–310.

[34] Yasmeen Hashish, Andrea Bunt, and James E Young. 2014. Involving children in content control: a collaborative and education-oriented content filtering approach. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems.* ACM, 1797–1806.

[35] Samantha Hautea, Sayamindu Dasgupta, and Benjamin Mako Hill. 2017. Youth perspectives on critical data literacies. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* ACM, 919–930.

[36] Alexis Hiniker, Hyewon Suh, Sabina Cao, and Julie A Kientz. 2016. Screen time tantrums: how families manage screen media experiences for toddlers and preschoolers. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* ACM, 648–660.

[37] Haiyan Jia, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Risk-taking As a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work &#38; Social Computing (CSCW '15).* ACM, New York, NY, USA, 583–599. https://doi.org/10.1145/2675133.2675287

[38] Steve Jones, Camille Johnson-Yale, Sarah Millermaier, and Francisco Seoane Pérez. 2009. US college students' Internet use: Race, gender and digital divides. *Journal of Computer-Mediated Communication* 14, 2 (2009), 244–264.

[39] Sharon Judge, Kimberly Floyd, and Tara Jeffs. 2015. Using mobile media devices and apps to promote young children's learning. In *Young Children and Families in the information age.* Springer, 117–131.

[40] Beeban Kidron, Anghrarad Rudkin, Miranda Wolpert, Joanna R. Adler, Andrew K. Przybylski, Elvira Perez Vallejos, Henrietta Bowden-Jones, Joshua J. Chauvin, Kathryn L. Mills, Marina Jirotka, and Julian Childs. 2017. *Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment.* Technical Report. 5Rights.

[41] Priya Kumar, Shalmali Milind naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2018. No Telling Passcodes Out Because They're Private?: Understanding Children's Mental Models of Privacy and Security Online. In *Proceedings of ACM Human-Computer Interaction (CSCW '18 Online First).* ACM.

[42] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th Annual ACM Conference on Interaction Design and Children (IDC'18). doi*, Vol. 10.

[43] Michael E Kummer and Patrick Schulte. 2016. When private information settles the bill: Money and privacy in Google's market for smartphone applications. *ZEW-Centre for European Economic Research Discussion Paper* 16-031 (2016).

[44] Sonia Livingstone. 2006. Children's privacy online: experimenting with boundaries within and beyond the family. (2006).

[45] Sonia Livingstone. 2018. Children: a special case for privacy? *Intermedia* 46, 2 (2018), 18–23.

[46] Sonia Livingstone, Alicia Blum-Ross, Jennifer Pavlick, and Kjartan Olafsson. 2018. *In the digital home, how do parents support their children and who supports them?* Technical Report. LSE.

[47] Sonia Livingstone, Alicia Blum-Ross, and Dongmiao Zhang. 2018. *What do parents think, and do, about their children's online privacy?* Technical Report. LSE.

[48] Sonia Livingstone, Julia Davidson, Joanne Bryce, Saqba Batool, Ciaran Haughton, and Anulekha Nandi. 2017. *Children's online activities, risks and safety: a literature review by the UKCCIS evidence group.* Technical Report. UKCCIS evidence group.

[49] Sonia Livingstone and Kjartan Olafsson. 2018. *When do parents think their child is ready to use the internet independently?* Technical Report. LSE.

[50] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2018. Conceptualising privacy online: what do, and what should, children understand? *Parenting for a Digital Future* (2018), 1–4.

[51] May O Lwin, Andrea JS Stanaland, and Anthony D Miyazaki. 2008. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing* 84, 2 (2008), 205–217.

[52] Sana Maqsood, Christine Mekhail, and Sonia Chiasson. 2018. A Day in the Life of Jos: A Web-based Game to Increase Children's Digital Literacy. In *Proceedings of the 17th ACM Conference on Interaction Design and Children.* ACM, 241–252.

[53] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* ACM, 523.

[54] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* ACM, 5197–5207.

[55] Linda Miller and Linda Pound. 2010. *Theories and approaches to learning in the early years.* Sage.

[56] Faye Mishna, Michael Saini, and Steven Solomon. 2009. Ongoing and online: Children and youth's perceptions of cyber bullying. *Children and Youth Services Review* 31, 12 (2009), 1222–1228.

[57] Myfanwy Morgan, Sara Gibbs, Krista Maxwell, and Nicky Britten. 2002. Hearing children's voices: methodological issues in conducting focus groups with children aged 7-11 years. *Qualitative research* 2, 1 (2002), 5–20.

[58] Michelle M Neumann and David L Neumann. 2014. Touch screen tablets and emergent literacy. *Early Childhood Education Journal* 42, 4 (2014), 231–239.

[59] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[60] ofcom.org. 2017. Children and parents: media use and attitude report. https://www.ofcom.org.uk/data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

[61] Kieron OHara. 2016. The Seven Veils of Privacy. *IEEE Internet Computing* 20, 2 (2016), 86–91.

[62] Luci Pangrazio and Neil Selwyn. 2017. 'My Data, My Bad ...': Young People's Personal Data Understandings and (Counter)Practices. In *Proceedings of the 8th International Conference on Social Media & Society (#SMSociety17).* ACM, New York, NY, USA, Article 52, 5 pages. https://doi.org/10.1145/3097286.3097338

[63] Stamatis Papadakis, Michail Kalogiannakis, and Nicholas Zaranis. 2016. Comparing tablets and PCs in teaching mathematics: an attempt to improve mathematics competence in early childhood education. *Preschool Prim. Educ* 4, 2 (2016), 241–253.

[64] Chris Quintana, Brian J Reiser, Elizabeth A Davis, Joseph Krajcik, Eric Fretz, Ravit Golan Duncan, Eleni Kyza, Daniel Edelson, and Elliot Soloway. 2004. A scaffolding design framework for software to support

science inquiry. *The journal of the learning sciences* 13, 3 (2004), 337–386.

[65] Irwin Reyes, Primal Wiesekera, Abbas Razaghpanah, Joel Reardon, Narseo Vallina-Rodriguez, Serge Egelman, and Christian Kreibich. 2017. "Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations. In *Workshop on Technology and Consumer Protection (ConPro 2017), in conjunction with the 38th IEEE Symposium on Security and Privacy.*

[66] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83.

[67] John Schacter and Booil Jo. 2016. Improving low-income preschoolers mathematics achievement with Math Shelf, a preschool tablet computer curriculum. *Computers in Human Behavior* 55 (2016), 223–229.

[68] Cristiana S. Silva, Glívia A.R. Barbosa, Ismael S. Silva, Tatiane S. Silva, Fernando Mourão, and Flávio Coutinho. 2017. Privacy for Children and Teenagers on Social Networks from a Usability Perspective: A Case Study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference (WebSci '17).* ACM, New York, NY, USA, 63–71. https://doi.org/10.1145/3091478.3091479

[69] Daniel J Solove. 2008. Understanding privacy. (2008).

[70] David W Stewart and Prem N Shamdasani. 2014. *Focus groups: Theory and practice.* Vol. 20. Sage publications.

[71] Matt Tierney and Lakshminarayanan Subramanian. 2014. Realizing privacy by definition in social networks. In *Proceedings of 5th Asia-Pacific Workshop on Systems.* ACM, 6.

[72] Max Van Kleek, Reuben Binns, Jun Zhao, and Nigel Shadbolt. [n. d.]. X-Ray Refine: Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps. In *Proceedings of 2018 CHI Conference on Human Factors in Computing Systems.* to appear.

[73] Rick Wash. 2010. Folk Models of Home Computer Security.. In *SOUPS.* 1–16.

[74] Margy Whalley. 2017. *Involving Parents in Their Children's Learning: A Knowledge-Sharing Approach.* Sage.

[75] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android Permissions Remystified: A Field Study on Contextual Integrity.. In *USENIX Security Symposium.* 499–514.

[76] Pamela Wisniewski. 2018. The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience? *IEEE Security & Privacy* 16, 2 (2018), 86–90.

[77] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing.* ACM, 51–69.

[78] Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences.. In *CSCW.* 523–540.

[79] Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk Models of Online Behavioral Advertising.. In *CSCW.* 1957–1969.

[80] Frances Zhang, Fuming Shih, and Daniel Weitzner. 2013. No surprises: measuring intrusiveness of smartphone applications by detecting objective context deviations. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society.* ACM, 291–296.

[81] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* (2017).

[82] Leah Zhang-Kennedy and Sonia Chiasson. 2016. Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge. In *Proceedings of the The 15th International Conference on Interaction Design and Children (IDC '16).* ACM, New York, NY, USA, 506–511. https://doi.org/10.1145/2930674.2935984

[83] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children.* ACM, 388–399.